Security at the COST of Productivity?

Presented by: Jim Ashmore
DoA, SITSD, Programs Office
406-444-2571

“It is difficult to keep up with all the changes in IT when the change happens so quickly.”

“We have limited resources (time, money, & people) to use against what seems to be an unlimited amount of forces & attempts to threaten and/or destroy delivery of our programs services.”

Productivity Enabling … ?

- How does one draw the line?
- What are the determining criteria?
- What do you watch out for?
- Are we spending more money enforcing than the risk warrants?
- How do we enable power users and maintain security?
- What is available to help this dilemma?

The Challenge Today …

- Coming to Terms
- Is the threat real, should I act?
- Define the characteristics / parameters
- An "A", "B", "C" approach
- An Exercise
- Components and tools for help
- Wrap - up

Coming to Terms …

- Architecture – the design applied to a program or process which constitutes the complete structure necessary to achieve the desired end-state
- HIPAA – Health Insurance Portability and Accountability Act
- Identity Management – identification of individuals in a system and how those individuals can access, visit, edit, read, browse, and more within that system
- Median – middle ground, center data point
- PII – Personally Identifiable Information, personal information the collection of which can be sensitive and create a vulnerability for identity theft when multiple pieces of this information can be gathered or obtained to establish an individual identity
- PPI – Protected Personal Information, personal information requiring protection by law, statute, program, or other regulatory constraint
- SDLC – Systems (or Software) Development Life Cycle, a process of creating or altering information systems, models, and methodologies.
- Sensitive Information – any form or medium where information can be transferred, stored, or obtained that is not intended for public access and requires control structures or processes to protect. This involves verbal/audible communications, hardcopy/printed files and records, as well as digital or electronic data.

Is the threat real, should I act?

Some numbers to consider…

- National Protected Personal Information Threats Reported
  - 2003-2008 over 41 Million CC/DC records hacked from only 9 brand name stores
  - Every lost record Avg cost is $138 to the organization who lost the record
  - 2008 over 313,000 filed identity theft complaints
  - 2009 over 278,000 filed identity theft complaints
- Montana Identity Theft Threats Reported
  - 2009 408 filed identity theft complaints
  - 2008 450 filed identity theft complaints
  - 2007 391 filed identity theft complaints
  - 2006 434 filed identity theft complaints
  - 2005 398 filed identity theft complaints
  - 2004 352 filed identity theft complaints
  - 2003 282 filed identity theft complaints
- Internal Breaches (employees)
  - 3 of 10 enterprise security threats are from internal sources
  - Insider fraud costs US enterprises over $600 Billion/yr
- 2008 Data Breaches Reported
  - 63% involved physical access
  - Only 37% were cyber breaches

Every day occurrences …

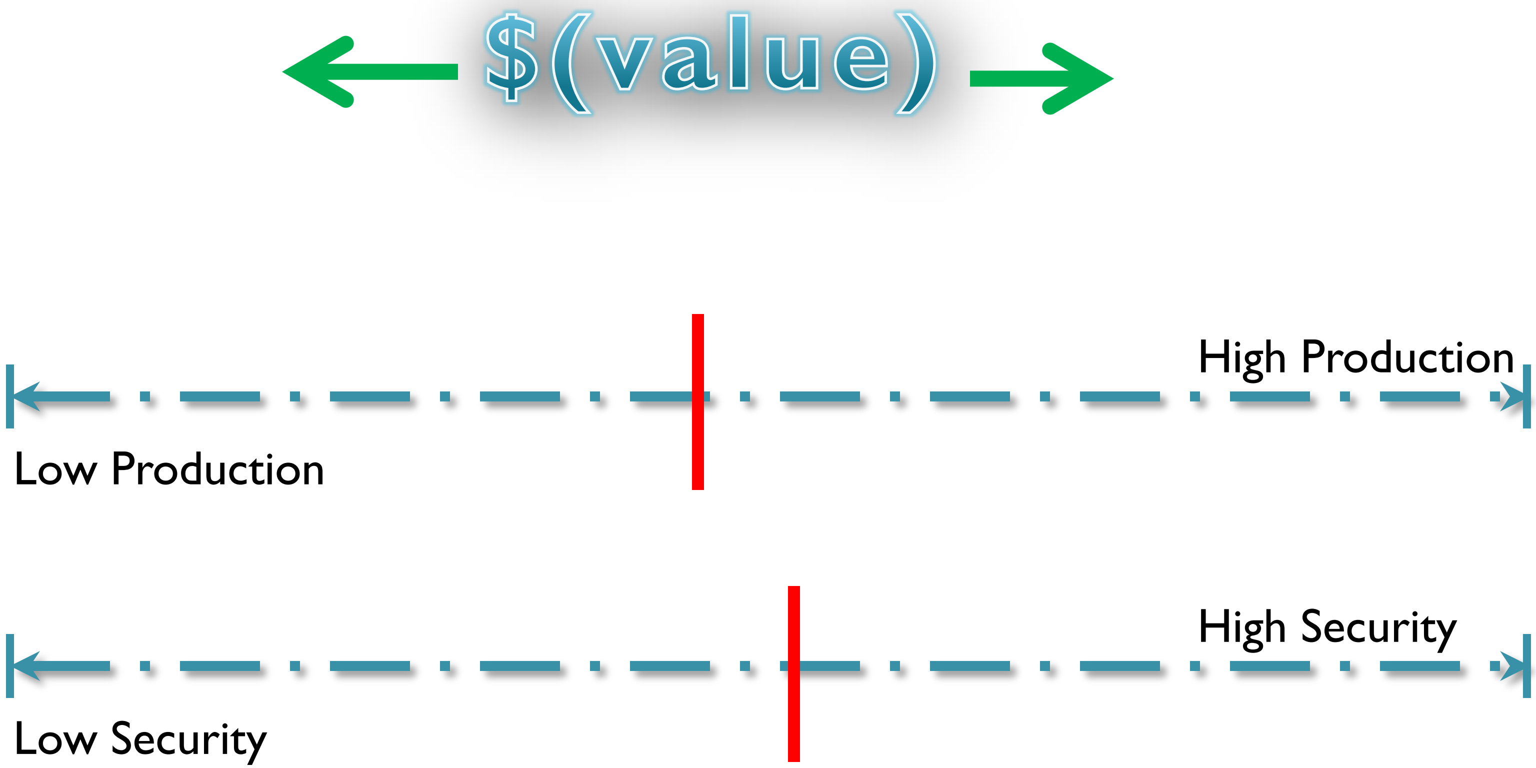
- The following sites provide regular updates on security information and breaches occurring almost every day:
  - epic.org = Electronic Privacy Information Center (Political and Legislative issues)
  - ftc.gov = Federal Trade Commission
  - privacyrights.com = Privacy Rights Clearinghouse (Alerts, Data Breaches, etc.)

The Threat is real …

- Montana government is open to attack
- One report states that 90% of public facing websites are vulnerable to attack
- What is Montana's vulnerability rating?
  - Rural small population density
  - Not in the industrial mainstream
  - Perception of value by the attacker

Define the characteristics / parameters

What are we dealing with in this Dilemma?



$(value)

High Production

Low Production

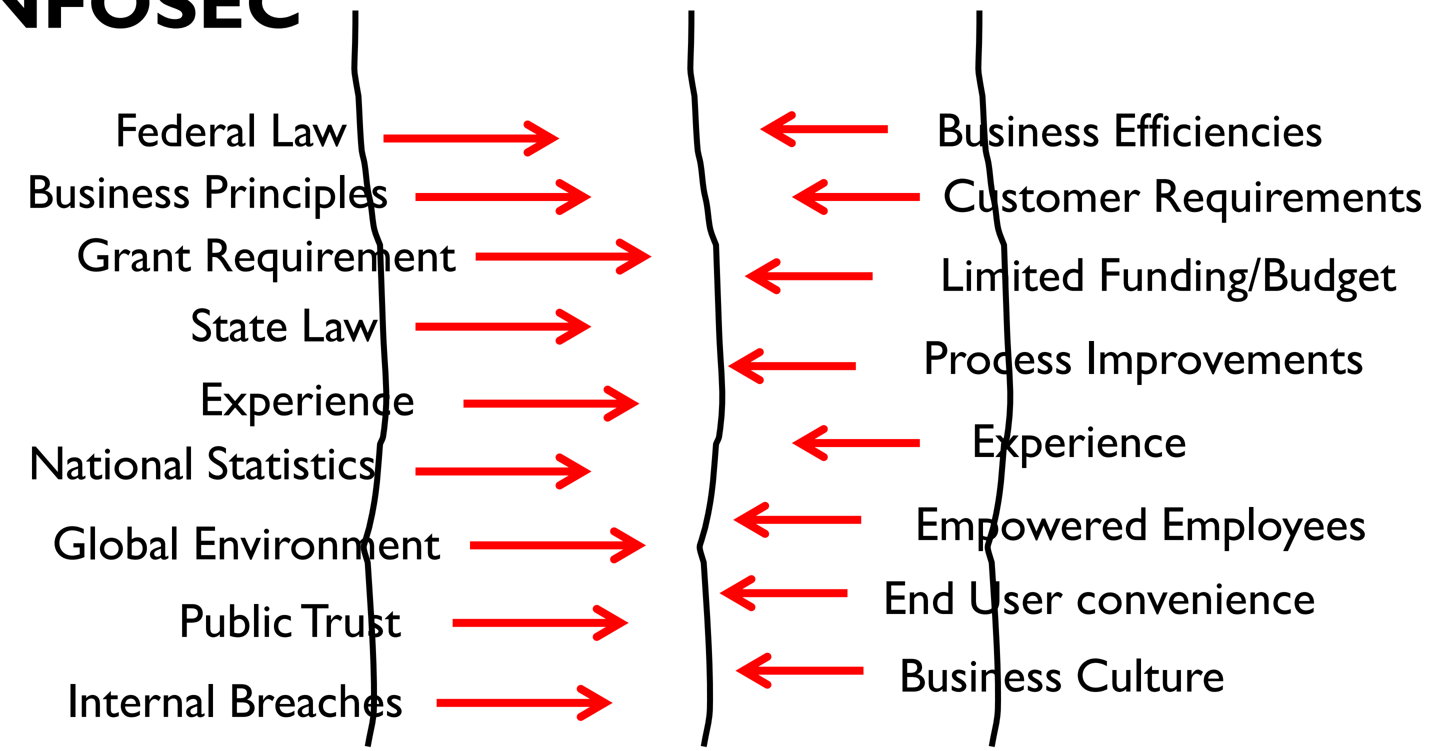
High Security

Low Security

Where does one draw the line between INFOSEC and ENABLING employees for continued or increased productivity?

$(value)

INFOSEC



Federal Law

Business Principles

Grant Requirement

State Law

Experience

National Statistics

Global Environment

Public Trust

Internal Breaches

Business Efficiencies

Customer Requirements

Limited Funding/Budget

Process Improvements

Experience

Empowered Employees

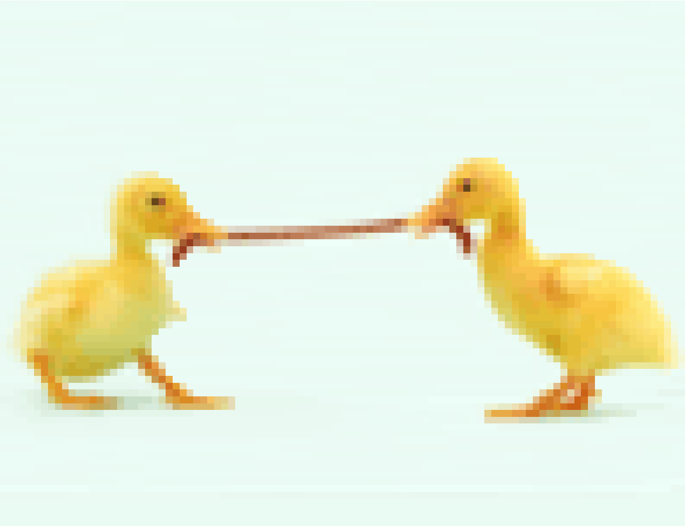
End User convenience

Business Culture

ENABLING Production

Where does one draw the line between INFOSEC and ENABLING employees for continued or increased productivity?

Tug – of – War …



Types of Information…

- PII – Personally Identifiable Information
  - First name
  - Last name
  - Home Address
  - Phone Number
  - Friends and family members
  - Work Address
  - Vehicle Registration plate
  - Date of Birth
  - Digital Identity/IP Address
  - Face, Fingerprints, or handwriting
  - Birthplace
  - Genetic Information
  - Criminal record
- PPI – Personal Protected Information
  - First and Last name
  - SSN
  - DL or State ID
  - Credit or Debit Card Number
  - Checking or Savings Acct Number (Financial Accounts)
  - Biometric information
  - Protected health information e.g., HIPAA data
  - Research involving human subjects
  - EDU-Transcripts, any cumulative listing of a student's grades

Types of Information…

- Sensitive Information
  - Intellectual Property
  - Proprietary Information
  - State Strategic Plans
  - Record Recovery Plans
  - Essential Records Plans
  - Other Federal, State, Local Government, or Grant identified sensitive information
- HIPAA
  - Patient Names
  - Street Address, city, county, zip code
  - Dates (except year) for dates related to an individual
  - E-mail, URLs, & IP #’s
  - Social security numbers
  - Account/Medical record #'s
  - Health plan beneficiary numbers
  - Certificate/license #'s
  - Vehicle id's & serial #'s
  - Device id's & serial #'s
  - Biometric identifiers
  - Full face images associated with HIPAA records
  - Any other unique identifying number, characteristic, or code
  - Payment Guarantor's information

Valid concerns …

- Stewards of Montana Governance
- Public Trust
- Potential for Loss of funds
- Criminal Event
- Operational Impact
- Embarrassment

Have we done our homework?

- This question has some implied assumptions that I would ask:
  - have we determined what our baseline position is, and
  - are we capturing quantifiable information to be able to measure performance to the baseline?
- Do we know our production rates?
- Do we know our efficiency rate?
- What is our capacity and are we at full capacity?

An "A", "B", "C" approach …

Can it be that simple?

Simple Security Scenario …

- Your Home

… is your castle

Breach controls and discipline …

Security is …

- A Weakest-Link Problem …

An A, B, C, approach …

A. Architecture with Frame of *the issue*
B. Business structure to manage the issue
C. Conquer; Implement and Monitor for adjustments and continued performance of operations or services

Risk Management Approach…

A. Architecture with Frame of the issue

   i. Risk Management Strategy - Considers the design, implementation, operation, and disposal of information systems and environments.

   ii. Identifies information requirements with associated assumptions, constraints, tradeoffs, priorities, vulnerabilities, likelihood, and threats.

   iii. Provides context and common perspective on how the organization manages risk; how to assess risk, respond to risk, and monitor risk.

Something to consider…

- Trade-offs?
- Prevention?
- Protection?
- SDLC Integration?
- Mandatory Controls?
- Strategic Plan & Budgetary Implications?

To what end … ?

INFOSEC Concepts

- Levels of access
  - How many layers before access to data/information? 1, 2, 3, or more?
  - What structure is best for my information?
- Types of controls (physical, technical, or administrative; preventive or detective)
  - Logon (User ID & Password) to Device; PC, Notebook, Network, e-mail, etc.
  - Encryption – document and/or system
  - Document Password Protected –
  - Physical Management/Control – Locked office/room/bldg
  - Sign-in/out records/files (manual or electronic)
  - Digital Signatures
- Other?

Risk Management Approach…cont’d

B. Business structure to manage the issue

  i. Define key roles responsible for the execution and management of this Architecture

  ii. Establish training criteria, skill sets and any certifications required for the type of information being controlled

  iii. Identify the operational and interactive hierarchy associated with this structure; chain of command, reporting requirements, etc.

Risk Management Approach…cont’d

C. Conquer; Implement and Monitor for adjustments and continued performance of operations or services

   i. Establish the implementation plan for training all staff, associated timelines, and coordination of any phasing requirements of the plan.

   ii. Report when full implementation is complete

   iii. Complete periodic reviews and updates on program execution

An Exercise Scenario…

Your Mission Today is …

- As CEO and Management Team you must prepare a product delivery plan for a contracted event to ensure safe and profitable event for your corporation
- Known Criteria:
  - Product = Ice-cream cones
  - Event = Contracted for community celebration; outdoors/park
  - Season = Summer, Forecasted Temp 80°f
  - Expected Attendance = 1,500 (enough cones so at least each attendee has one)
- Report to Board Recommendations

Mission UPDATE …

- Your Sales staff are on location, at event
- Weather report: weather advisory, winds up to 30 MPH expected with 60% chance of rain, temperature should drop to 65°F
- Event Manager: event will continue as planned, make appropriate accommodations to fulfill contract.

Components and tools for help …

2005 active year for PII protection Federal Legislation initiatives …

- Privacy Act of 2005
- Information Protection and Security Act
- Identity Theft Prevention Act of 2005
- Online Privacy Protection Act of 2005
- Anti-phishing Act of 2005
- Social Security Number Protection Act of 2005
- What happened to these…?

What can help … ?

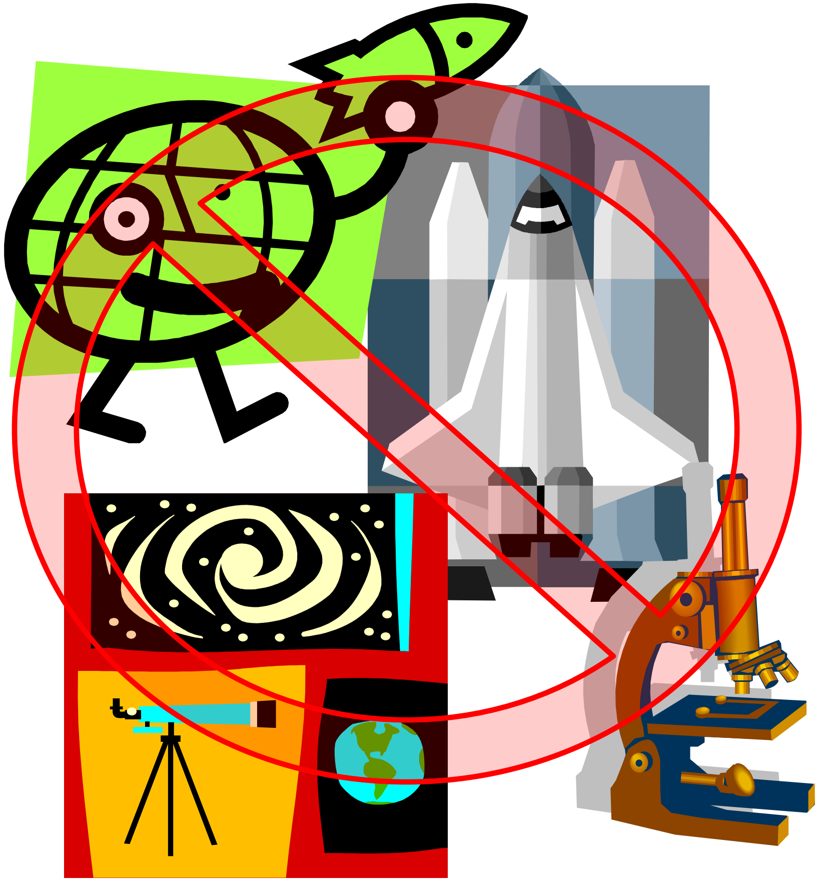
- Team effort working together, e.g., ISMG
  - Sharing Best Practices
- Assistance from Programs Office
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- DHS Handbook for Safeguarding Sensitive Personally Identifiable Information (PII), 10-06-2011
-

Wrap - up …

This should not be an ELEPHANT TASK.

Don’t bite off more than you can chew.

This should not be a SCIENCE Project.



Wrap - up …

This should be as simple as A, B, C:

Architecture
Business structure
Conquer

The End…

- Questions